Zdôvodnenie strategickosti národného projektu „Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe“

Hlavným cieľom národného systému riadenia incidentov kybernetickej bezpečnosti vo VS je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej aj „jednotky CSIRT“) pre podsektor Informačné systémy verejnej správy podľa prílohy č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti“). **Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe** predstavuje prvú strategickú fázu budovania **celonárodného systému riadenia incidentov kybernetickej bezpečnosti**. Prostredníctvom tejto fázy budovania celonárodného systému budú pokryté preventívne a reaktívne služby pre podsektor Informačné systémy verejnej správy (ďalej aj „ISVS“).

Projekt je navrhnutý ako národný projekt, ktorého cieľovou skupinou sú tieto zainteresované strany:

- prevádzkovatelia jednotiek CSIRT zapojené do národného systému,
- prevádzkovatelia informačných systémov verejnej správy v konštituencii (resp. „jurisdikcii“) jednotlivých jednotiek CSIRT.

Tento projekt v kontexte NKIVS prispieva k realizácii priority informatizácie verejnej správy „Formovanie infraštruktúry“ a je plne v súlade so všetkými tromi strategickými cieľmi „prevencia“, „pripravenosť“ a „udržateľnosť“ Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike, ktorú odkazuje NKIVS. V rámci OPII projekt prispieva k naplneniu výsledkov špecifického cieľa 7.9 „Zvýšenie kybernetickej bezpečnosti v spoločnosti“, ktorými sú:

- zníženie finančných dopadov a dopadov na inštitúcie verejnej správy pri bezpečnostných incidentoch,
- zvýšenie vyspelosti trhu s bezpečnostnými riešeniami zvýšením výdavkov na bezpečnosť verejného sektora,
- zvýšenie kybernetickej bezpečnosti a aplikovanie najnovších poznatkov v európskom priestore,
- zvýšenie miery inovácie v oblasti bezpečnostných opatrení,
- zvýšenie dôvery občanov a podnikateľov v digitálny priestor,
- zvýšenie transparentnosti pri riešení bezpečnostných incidentov a kybernetických útokov.

Projekt je taktiež plne v súlade i so zásadným dokumentom kybernetickej bezpečnosti Slovenskej republiky Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schváleným vládou SR.

Komplexné zabezpečenie kybernetickej bezpečnosti v rámci jednotlivých vecných oblastí musí pokryť výkon verejnej moci a výkon odborných činností. Pre naplnenie tohto ambiciózneho a náročného cieľa je potrebné zásadne posilniť a rozšíriť jednotky CSIRT, ktoré budú súčasťou národného systému a technicky i organizačne zabezpečiť ich komunikáciu. Úlohou jednotiek CSIRT je vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch národnej jednotke CSIRT a vládnej jednotke CSIRT. Štruktúra jednotiek CSIRT, ktoré budú súčasťou projektu bola navrhnutá tak, aby bolo možné efektívne poskytovať preventívne a reaktívne služby definované v § 15 zákona o kybernetickej bezpečnosti pre podsektor ISVS.

Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe budú tvoriť tieto jednotky CSIRT:

- SK-CERT – národná jednotka CSIRT, ktorej prevádzkovateľom je Národný bezpečnostný úrad,
- CSIRT.SK – vládna jednotka CSIRT v pôsobnosti ÚPPVII, ktorá je súčasne jednotkou CSIRT pre podsektor ISVS,
- CSIRT SIS – sektorová jednotka CSIRT v pôsobnosti Slovenskej informačnej služby, ktorá zabezpečuje spravodajské činnosti kybernetickej bezpečnosti pre podsektor ISVS,
- GOV CERT SK – jednotka CSIRT zriadená Národnou agentúrou pre sieťové a elektronické služby, prevádzkovateľom základnej služby zabezpečujúca činnosti kybernetickej bezpečnosti pre kľúčové stavebné prvky e-Governmentu, ktorými sú Ústredný portál verejnej správy a vládna sieť Govnet.

Je dôležité poznamenať, že v ďalších fázach rozširovania celonárodného systému sa uvažuje so zapojením ďalších sektorových jednotiek CSIRT v gescii príslušných ústredných orgánov podľa zákona o kybernetickej bezpečnosti, ktoré môžu zvýšenie vlastnej vyspelosti riešiť či už prostredníctvom národných projektov alebo dopytovo-orientovaných výziev.

Z pohľadu samotného technického vybavenia jednotiek CSIRT si je potrebné uvedomiť, že sa jedná o vysoko špecifické hardvérové a softvérové vybavenie, ktorého primárnou úlohou je poskytovať nástroj na poskytovanie preventívnych a reaktívnych služieb v zmysle zákona o kybernetickej bezpečnosti. V tejto súvislosti možno konštatovať, že projekt si vyžiada zvýšené finančné nároky na hardvérové vybavenie, nakoľko významná množina technického vybavenia predstavuje tzv. appliance (mix hardvéru a softvéru dodávaný ako jedno celistvé black-box riešenie, príkladom môže byť: https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/ alebo https://en.wikipedia.org/wiki/Security_appliance).

V tomto prípade sa bude musieť z pohľadu účtovného na technické vybavenie pozerať ako na hardvér a to aj napriek tomu, že softvér inštalovaný v rámci appliance predstavuje prevažnú časť hodnoty zariadenia. Ďalšiu nezanedbateľnú množinu budú tvoriť prenosné hardvérové zariadenia, ktoré budú slúžiť na výkon penetračného testovania či forenznej analýzy priamo v teréne. Čo sa týka možností využitia kapacít vládneho cloudu možno konštatovať, že vzhľadom na povahu technického vybavenia jednotlivých jednotiek CSIRT nebude možné z prevádzkového (pre výkon bezpečnostných funkcií je potrebné mať aj lokálne dostupný HW a SW) a bezpečnostného (napr. nie je vhodné analyzovať nebezpečný kód na zdrojoch vládneho cloudu, lebo tu hrozí riziko nákazy) hľadiska využiť túto možnosť.

Z vyššie uvedeného vyplýva, že tento projekt si vyžiada množstvo hardvérového vybavenia presahujúce 30 % z celkového objemu oprávnených výdavkov projektu, avšak z pohľadu strategickosti a národného významu projektu je takéto rozloženie hardvérových a softvérových komponentov nevyhnutné.